Asymmetric quantum convolutional codes

Giuliano G. La Guardia *

October 14, 2016

Abstract

In this paper, we construct the first families of asymmetric quantum convolutional codes (AQCC)'s. These new AQCC's are constructed by means of the CSS-type construction applied to suitable families of classical convolutional codes, which are also constructed here. The new codes have noncatastrophic generator matrices and they have great asymmetry. Since our constructions are performed algebraically, i.e., we develop general algebraic methods and properties to perform the constructions, it is possible to derive several families of such codes and not only codes with specific parameters. Additionally, several different types of such codes are obtained.

Index Terms – **convolutional codes, quantum convolutional codes**

1 Introduction

Several works available in literature deal with constructions of quantum error-correcting codes (QECC, for short) and asymmetric quantum error-correcting codes (AQECC) [5, 24, 4, 13, 11, 14, 29, 15, 16, 17]. In contrast with this subject of research one has the theory of quantum convolutional codes [25, 26, 1, 9, 2, 3, 7, 18, 19]. Ollivier and Tillich [25, 26] were the first to develop the stabilizer structure for these codes. Almeida and Palazzo Jr. constructed an $[(4, 1, 3)]$ (memory $\mu = 3$) quantum convolutional code [1]. Grassl and Rötteler [8, 9] generated quantum convolutional codes as well as they provide algorithms to obtain non-catastrophic encoders. Forney *et al.* constructed rate $(n-2)/n$ quantum convolutional codes.

An asymmetric quantum convolutional code (AQCC) is a quantum code defined over quantum channels where qudit-flip errors and phase-shift errors may have different probabilities. As it is well known, Steane [31] was the first who introduced the notion of asymmetric quantum errors. The parameters of an AQCC will be denoted by $[(n, k, \mu; \gamma, [d_z]_f/[d_x]_f)]_q$, where n is the frame size, k is the number of logical qudits per frame, μ is the memory, $[d_z]_f$ ($[d_x]_f$) is the

*Giuliano Gadioli La Guardia is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil.

free distance corresponding to phase-shift (qudit-flip) errors and γ is the degree of the code. The combined amplitude damping and dephasing channel (see [29] the references therein) is a quantum channel whose probability of occurrence of phase-shift errors is greater than the probability of occurrence of qudit-flip errors.

In this paper we propose constructions of the first families of asymmetric quantum convolutional codes. The constructions presented here are performed algebraically (as mentioned above).

The first families of AQCC's presented in this paper, i.e., Construction I, are obtained from the construction method proposed in Subsection 3.1. This construction method is general, i.e., it holds for every choice of sets of $m < n$ linearly independent vectors $\mathbf{v}_i \in \mathbb{F}_q^n$, $i = 1, 2, \ldots, m$ (see the proof of Theorem 3.1). The AQCC's derived from Construction I have parameters

- $[(n, \operatorname{rk} H_0, \mu^*; \gamma_1 + \gamma_2, (d_z)_f/(d_x)_f)]_q$,
  where $\gamma_1 = \mu(\operatorname{rk} H_\mu + \operatorname{rk} H_\mu^{'}) + \sum_{i=1}^{\mu-1}(\mu - i)[\operatorname{rk} H_{(\mu-i)}^{'} - \operatorname{rk} H_{(\mu-i+1)}^{'}]$, $\gamma_2 = \mu(\operatorname{rk} H_\mu^{'}) + \sum_{i=1}^{\mu-1}(\mu - i)[\operatorname{rk} H_{(\mu-i)}^{'} - \operatorname{rk} H_{(\mu-i+1)}^{'}]$, $(d_x)_f \geq (d_1)_f \geq d^\perp$ and $(d_z)_f \geq (d_2)_f^\perp$, where $(d_1)_f, d^\perp, (d_2)_f^\perp$ and the matrices $H_0, H_0^{'}, H_1, H_1^{'}, \ldots, \ldots, H_\mu, H_\mu^{'}$ are defined in the proof of Theorem 3.1.

In Construction II (see Subsection 3.2) we present families of AQCC's derived from classical maximum-distance-separable BCH codes:

- $[(n, 2i - 4, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$,
  where $q = 2^t$, $t \geq 4$, $n = q + 1$, $(d_z)_f \geq n - 2i - 1$ and $(d_x)_f \geq 3$, for all $3 \leq i \leq \frac{q}{2} - 1$;
- $[(n, 2i - 2t - 2, \mu^*; 6, [d_z]_f \geq n - 2i - 1/[d_x]_f \geq 2t + 3)]_q$,
  where $q = 2^l$, $l \geq 4$, $n = q + 1$, t integer with $1 \leq t \leq i - 2$, $3 \leq i \leq \frac{q}{2}$;
- $[(n, 2i - 2t, \mu^*; 4, [d_z]_f/[d_x]_f)]_q$,
  where $(d_z)_f \geq n - 2i - 1$ and $(d_x)_f \geq 2t + 3$, $q = 2^l$, $l \geq 4$, $n = q + 1$, t integer with $1 \leq t \leq i - 1$, $2 \leq i \leq \frac{q}{2}$;
- $[(n, 2i - 2t - 2, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$,
  where $q = p^l$, p is an odd prime, $l \geq 2$, $n = q + 1$, $(d_z)_f \geq n - 2i$ and $(d_x)_f \geq 2t + 2$, for all $1 \leq t \leq i - 2$, where $3 \leq i \leq \frac{n}{2} - 1$;
- $[(n, 2i - 2t, \mu^*; 4, [d_z]_f/[d_x]_f)]_q$,
  where $q = p^l$, p is an odd prime, $l \geq 2$, $n = q + 1$, $(d_z)_f \geq n - 2i$ and $(d_x)_f \geq 2t + 2$, for all $1 \leq t \leq i - 1$, with $2 \leq i \leq \frac{n}{2} - 1$;

In Construction III (see Subsection 3.3) we construct families of AQCC's derived from classical Reed-Solomon and generalized Reed-Solomon codes. The

AQCC's shown in Construction II are distinct of the AQCC's shown in Construction III.

- $[(q-1, i-t-1, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$,
  where $q \geq 8$ is a prime power $(d_z)_f \geq q-i-1$ and $(d_x)_f \geq t+2$, for all $1 \leq t \leq i-2$, where $3 \leq i \leq q-3$;

- $[(q-1, i-t, \mu^*; 2, [d_z]_f/[d_x]_f)]_q$,
  where $(d_z)_f \geq q-i-1$, $(d_x)_f \geq t+2$, for all $1 \leq t \leq i-1$, where $2 \leq i \leq q-3$;

- $[(n, n-t-k-2, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$,
  where $(d_z)_f \geq t+2$ and $(d_x)_f \geq k+1$, where $q \geq 5$ is a prime power, $k \geq 1$ and n are integers such that $5 \leq n \leq q$ and $k \leq n-4$ and t is an integer with $1 \leq t \leq n-k-2$;

- $[(n, n-t-k-1, \mu^*; 2, [d_z]_f/[d_x]_f)]_q$,
  where $q \geq 5$ is a prime power, $k \geq 1$, $n \geq 5$ are integers such that $n \leq q$, $k \leq n-4$, $1 \leq t \leq n-k-1$, $(d_z)_f \geq t+2$ and $(d_x)_f \geq k+1$.

The ideas utilized in Constructions II and III are very similar to that shown in Construction I, although in the latter constructions it is possible to compute precisely the parameters are of the AQCC's due to the structure of the classical BCH codes and (generalized) Reed-Solomon codes involved in the construction process.

The paper is arranged as follows. In Section 2, we recall the concepts of convolutional and quantum convolutional codes. In Section 3, we present the contributions of this work, *i.e.*, the first families of asymmetric quantum convolutional codes are constructed. In Section 4, we discuss the results presented in this paper and, in Section 5, the final remarks are drawn.

2 Background

Notation. Throughout this paper, p denotes a prime number, q is a prime power and $\mathbb{F}_q$ is a finite field with q elements. The code length is denoted by n and we always assume that $\gcd(q, n) = 1$. As usual, the multiplicative order of q modulo n is denoted by $l = \mathrm{ord}_n(q)$, and α is considered a primitive n-th root of unity in the extension field $\mathbb{F}_{q^l}$. The parameters of a linear block code over $\mathbb{F}_q$, of length n, dimension k and minimum distance d, is denoted by $[n, k, d]_q$. Sometimes, we abuse the notation by writing $C = [n, k, d]_q$. If C is a linear code then $C^\perp$ denotes its Euclidean dual.

2.1 Review of Convolutional Codes

Convolutional codes are extensively investigated in the literature [6, 20, 27, 28, 12, 10, 30]. Recall that a polynomial encoder matrix $G(D) \in \mathbb{F}_q[D]^{k \times n}$ is called

basic if $G(D)$ has a polynomial right inverse. A basic generator matrix is called *reduced* (or minimal, see [30, 10]) if the overall constraint length $\gamma = \sum_{i=1}^{k} \gamma_i$, where $\gamma_i = \max_{1 \leq j \leq n}\{\deg g_{ij}\}$, has the smallest value among all basic generator matrices. In this case, we say that γ is the *degree* of the resulting code.

A rate k/n *convolutional code* C with parameters $(n, k, \gamma; \mu, d_f)_q$ is a submodule of $\mathbb{F}_q[D]^n$ generated by a reduced basic matrix $G(D) = (g_{ij}) \in \mathbb{F}_q[D]^{k \times n}$, *i.e.*, $C = \{\mathbf{u}(D)G(D) | \mathbf{u}(D) \in \mathbb{F}_q[D]^k\}$, where n is the length, k is the dimension, $\gamma = \sum_{i=1}^{k} \gamma_i$ is the degree, $\mu = \max_{1 \leq i \leq k}\{\gamma_i\}$ is the memory and $d_f = \mathrm{wt}(C) = \min\{wt(\mathbf{v}(D)) \mid \mathbf{v}(D) \in C, \mathbf{v}(D) \neq 0\}$ is the free distance of the code. In the above definition, the *weight* of an element $\mathbf{v}(D) \in \mathbb{F}_q[D]^n$ is defined as $\mathrm{wt}(\mathbf{v}(D)) = \sum_{i=1}^{n} \mathrm{wt}(v_i(D))$, where $\mathrm{wt}(v_i(D))$ is the number of nonzero coefficients of $v_i(D)$. In the field of Laurent series $\mathbb{F}_q((D))$, whose elements are given by $\mathbf{u}(D) = \sum_i u_i D^i$, where $u_i \in \mathbb{F}_q$ and $u_i = 0$ for $i \leq r$, for some $r \in \mathbb{Z}$, we define the weight of $\mathbf{u}(D)$ as $\mathrm{wt}(\mathbf{u}(D)) = \sum_{\mathbb{Z}} \mathrm{wt}(u_i)$. A generator matrix $G(D)$ is called *catastrophic* if there exists a $\mathbf{u}(D)^k \in \mathbb{F}_q((D))^k$ of infinite Hamming weight such that $\mathbf{u}(D)^k G(D)$ has finite Hamming weight. The AQCC's constructed in this paper have noncatastrophic generator matrices since the corresponding classical convolutional codes constructed here have basic (and reduced) generator matrices. The Euclidean inner product of two n-tuples $\mathbf{u}(D) = \sum_i \mathbf{u}_i D^i$ and $\mathbf{v}(D) = \sum_j \mathbf{u}_j D^j$ in $\mathbb{F}_q[D]^n$ is defined as $\langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = \sum_i \mathbf{u}_i \cdot \mathbf{v}_i$. If C is a convolutional code then the code $C^\perp = \{\mathbf{u}(D) \in \mathbb{F}_q[D]^n \mid \langle \mathbf{u}(D) \mid \mathbf{v}(D) \rangle = 0 \text{ for all } \mathbf{v}(D) \in C\}$ denotes its Euclidean dual.

Let $C \subseteq \mathbb{F}_q^n$ an $[n, k, d]_q$ block code with parity check matrix H. We split H into $\mu + 1$ disjoint submatrices H_i such that $H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_\mu \end{bmatrix}$, where each H_i has n columns, obtaining the polynomial matrix $G(D) = \tilde{H}_0 + \tilde{H}_1 D + \tilde{H}_2 D^2 + \ldots + \tilde{H}_\mu D^\mu$. The matrices $\tilde{H}_i$, $1 \leq i \leq \mu$, are derived from the respective matrices H_i by adding zero-rows at the bottom such that $\tilde{H}_i$ has κ rows in total, where κ is the maximal number of rows among the matrices H_i. The matrix $G(D)$ generates a convolutional code V.

Theorem **2.1** *[2, Theorem 3] Let $C \subseteq \mathbb{F}_q^n$ be a linear code with parameters $[n, k, d]_q$. Assume that $H \in \mathbb{F}_q^{(n-k) \times n}$ is a parity check matrix for C partitioned into submatrices $H_0, H_1, \ldots, H_\mu$ as above such that $\kappa = \mathrm{rk}\, H_0$ and $\mathrm{rk}\, H_i \leq \kappa$ for $1 \leq i \leq \mu$.*
(a) The matrix $G(D)$ is a reduced basic generator matrix;

(b) If d_f and $d_f^\perp$ denote the free distances of V and $V^\perp$, respectively, d_i denote the minimum distance of the code $C_i = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{v}\tilde{H}_i^t = 0\}$ and $d^\perp$ is the minimum distance of $C^\perp$, then one has $\min\{d_0 + d_\mu, d\} \leq d_f^\perp \leq d$ and $d_f \geq d^\perp$.

2.2 Review of quantum convolutional codes

In this subsection, we recall the concept of quantum convolutional code (QCC). For more details, the reader can consult [2, 3, 7].

A quantum convolutional code is defined by means of its stabilizer which is a subgroup of the infinite version of the Pauli group, consisting of tensor products of generalized Pauli matrices acting on a semi-infinite stream of qudits. The stabilizer can be defined by a stabilizer matrix of the form $S(D) = (X(D) \mid Z(D)) \in \mathbb{F}_q[D]^{(n-k)\times 2n}$ satisfying $X(D)Z(1/D)^t - Z(D)X(1/D)^t = 0$ (symplectic orthogonality). Let $\mathcal{Q}$ be a QCC defined by a full-rank stabilizer matrix $S(D)$ given above. The constraint length is defined as $\gamma_i = \max_{1\leq j\leq n}\{\max\{\deg X_{ij}(D),\ \deg Z_{ij}(D)\}\}$, and the overall constraint length as $\gamma = \sum_{i=1}^{n-k} \gamma_i$. If γ has the smallest value among all basic generator matrices then γ is the *degree* of the code. The memory μ of $\mathcal{Q}$ is defined as $\mu = \max_{1\leq i\leq n-k, 1\leq j\leq n}\{\max\{\deg X_{ij}(D),\ \deg Z_{ij}(D)\}\}$.

Here we define the free distance of a quantum convolutional code [3]. Let $\mathbb{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$ be the Hilbert space and $|x\rangle$ be the vectors of an orthonormal basis of $\mathbb{C}^q$, where $x \in \mathbb{F}_q$. Let $a, b \in \mathbb{F}_q$ and take the unitary operators $X(a)$ and $Z(b)$ in $\mathbb{C}^q$ defined by $X(a)|x\rangle = |x + a\rangle$ and $Z(b)|x\rangle = w^{tr(bx)}|x\rangle$, respectively, where $w = \exp(2\pi i/p)$ is a primitive p-th root of unity, p is the characteristic of $\mathbb{F}_q$ and tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Let $\mathbb{E} = \{X(a), Z(b) | a, b \in \mathbb{F}_q\}$ be the *error basis*. The set P_∞ (according to [3]) is the set of all infinite tensor products of matrices $N \in \langle M \mid M \in \mathbb{E}\rangle$, in which all but finitely many tensor components are equal to I, where I is the $q \times q$ identity matrix. Then one defines the *weight* wt of $A \in P_\infty$ as its (finite) number of nonidentity tensor components. In this context, one says that a quantum convolutional code has free distance d_f if and only if it can detect all errors of weight less than d_f, but cannot detect some error of weight d_f. Then $\mathcal{Q}$ is a rate k/n code with parameters $[(n, k, \mu; \gamma, d_f)]_q$, where n is the frame size, k is the number of logical qudits per frame, μ is the memory, γ is the degree and d_f is the free distance of the code.

On the other hand, a quantum convolutional code can also be described in terms of a semi-infinite stabilizer matrix S with entries in $\mathbb{F}_q \times \mathbb{F}_q$ in the following way. If $S(D) = \sum_{i=0}^{\mu} G_i D^i$, where each matrix G_i for all $i = 0, \ldots, \mu$,

is a matrix of size $(n-k)\times n$, then the semi-infinite matrix is defined as

$$S=\begin{bmatrix} G_0 & G_1 & \dots & G_\mu & 0 & \dots & \dots & \dots \\ 0 & G_0 & G_1 & \dots & G_\mu & 0 & \dots & \dots \\ 0 & 0 & G_0 & G_1 & \dots & G_\mu & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

Let us recall the well known CSS-like construction:

Theorem **2.2** *[31, 5, 13] (CSS-like Construction) Let C_1 and C_2 be two classical convolutional codes with parameters $(n,k_1)_q$ and $(n,n-k_2)_q$, respectively, such that $C_2^{\perp}\subset C_1$. The stabilizer matrix is given by*

$$\left(\begin{array}{c|c} H_2(D) & 0 \\ 0 & H_1(D) \end{array}\right)\in \mathbb{F}_q[D]^{(n-k_1+k_2)\times 2n},$$

where $H_1(D)$ and $H_2(D)$ denote parity check matrices of C_1 and C_2, respectively. Then there exists an $[(n,K=k_1-k_2,(d_z)_f/(d_x)_f)]_q$ convolutional stabilizer code, where $(d_x)_f=\min\{\mathrm{wt}(C_1\backslash C_2^{\perp}),\mathrm{wt}(C_2\backslash C_1^{\perp})\}$ and $(d_z)_f=\max\{\mathrm{wt}(C_1\backslash C_2^{\perp}),\mathrm{wt}(C_2\backslash C_1^{\perp})\}$.

Remark **2.3** *To avoid overly burdensome notation, we assume throughout this paper that if $(d_x)_f>(d_z)_f$ then the values are changed.*

3 Asymmetric quantum convolutional codes

In this section we present the contributions of this paper. As it was said previously, we construct the first families of AQCC's by means of algebraic methods. More specifically, we construct reduced basic generator matrices for two classical convolutional codes V_1 and V_2, where $V_2\subset V_1$, in order to apply the CSS-type construction. This section is divided in three subsections, which contain three distinct code constructions.

3.1 Construction I

In this section we present the first construction method of this paper. Theorem 3.1 establishes the existence of AQQCs:

Theorem **3.1** *(General Construction) Let q be a prime power and n be a positive integer. Then there exist asymmetric quantum convolutional codes with parameters*

$$[(n,\mathrm{rk}\,H_0,\mu^*;\gamma_1+\gamma_2,(d_z)_f/(d_x)_f)]_q,$$

where $\gamma_1=\mu(\mathrm{rk}\,H_\mu+\mathrm{rk}\,H_\mu^{'})+\sum_{i=1}^{\mu-1}(\mu-i)[\mathrm{rk}\,H_{(\mu-i)}^{'}-\mathrm{rk}\,H_{(\mu-i+1)}^{'}]$, $\gamma_2=\mu(\mathrm{rk}\,H_\mu^{'})+\sum_{i=1}^{\mu-1}(\mu-i)[\mathrm{rk}\,H_{(\mu-i)}^{'}-\mathrm{rk}\,H_{(\mu-i+1)}^{'}]$, $(d_x)_f\geq(d_1)_f\geq d^{\perp}$ *and* $(d_z)_f\geq(d_2)_f^{\perp}$,

where $(d_1)_f, d^{\perp}, (d_2)_f^{\perp}$ *and the matrices* $H_0, H_0^{'}, H_1, H_1^{'}, \ldots, H_\mu, H_\mu^{'}$, *are constructed below.*

Proof: Consider a set of $m < n$ linearly independent (LI) vectors $\mathbf{v}_i \in \mathbb{F}_q^n$, $i = 1, 2, \ldots, m$. Let

$$\mathcal{H} = \begin{bmatrix} H_0 \\ H_0^{'} \\ H_1 \\ H_1^{'} \\ \vdots \\ H_\mu \\ H_\mu^{'} \end{bmatrix}$$

be the matrix whose rows are the vectors $\mathbf{v}_i$, $i = 1, 2, \ldots, m$. The matrices $H_0, H_0^{'}, H_1, H_1^{'}, \ldots, H_\mu, H_\mu^{'}$, are mutually disjoint. The matrices H_i, $i = 0, 1, \ldots, \mu$, are chosen in such a way that $\operatorname{rk} H_i = \operatorname{rk} H_j$, for all $i, j = 0, 1, \ldots, \mu$ (the choice of the vectors in each H_i is arbitrary). In order to compute the degree of the convolutional code constructed in the sequence, we assume that $H_0^{'}$ has full rank and $\operatorname{rk} H_0^{'} \geq \operatorname{rk} H_1^{'} \geq \ldots \geq \operatorname{rk} H_\mu^{'}$. The matrices $\tilde{H}_i^{'}$ with $1 \leq i \leq \mu$, are obtained from the respective matrices $H_i^{'}$ by adding zero-rows at the bottom such that $\tilde{H}_i$ has $\operatorname{rk} H_0^{'}$ rows in total.

Let $\mathcal{H}$ be a parity check matrix of a linear block code $C = [n, k, d]_q$, where $k = n - m$. Consider the linear block code $C^* = [n, k^*, d^*]_q$ with parity check matrix

$$H^* = \begin{bmatrix} H_0^{'} \\ H_1^{'} \\ \vdots \\ H_\mu^{'} \end{bmatrix}.$$

Next, we construct a matrix $G_1(D)$ as follows:

$$G_1(D) = \begin{bmatrix} H_0 \\ -- \\ H_0^{'} \end{bmatrix} + \begin{bmatrix} H_1 \\ -- \\ \tilde{H}_1^{'} \end{bmatrix} D + \begin{bmatrix} H_2 \\ -- \\ \tilde{H}_2^{'} \end{bmatrix} D^2 + \ldots + \begin{bmatrix} H_\mu \\ -- \\ \tilde{H}_\mu^{'} \end{bmatrix} D^\mu.$$

Further, let us consider the submatrices $G_0(D)$ and $G_2(D)$ of $G_1(D)$, given, respectively, by

$$G_0(D) = H_0 + H_1 D + H_2 D^2 + \ldots + H_\mu D^\mu$$

and

$$G_2(D) = H_0^{'} + \tilde{H}_1^{'} D + \tilde{H}_2^{'} D^2 + \ldots + \tilde{H}_\mu^{'} D^\mu.$$

We know that $G_1(D) \in \mathbb{F}_q[D]^{\kappa \times n}$, *i.e.*, $G_1(D)$ has full rank $\kappa = \operatorname{rk} H_0 + \operatorname{rk} H_0^{'}$; $G_2(D)$ has full rank $k_0^{'} = \operatorname{rk} H_0^{'}$. From construction, it follows that $G_1(D)$ and

$G_2(D)$ are reduced basic generator matrices of convolutional codes V_1 and V_2, respectively. Both convolutional codes have memory μ. Applying a similar idea as in the proof of [2, Theorem 3], the free distance $(d_1)_f$ of the convolutional code V_1 and the free distance $(d_1)_f^{\perp}$ of its Euclidean dual $V_1^{\perp}$ satisfy $\min\{D_0 + D_\mu, d\} \leq (d_1)_f^{\perp} \leq d$ and $(d_1)_f \geq d^{\perp}$, where D_0 is the minimum distance of the code with parity check matrix $\begin{bmatrix} H_0 \\ -- \\ H_0^{'} \end{bmatrix}$ and D_μ is the minimum distance of the code with parity check matrix $\begin{bmatrix} H_\mu \\ -- \\ \tilde{H}_\mu^{'} \end{bmatrix}$. Similarly, the free distance $(d_2)_f$ of V_2 and the free distance $(d_2)_f^{\perp}$ of $V_2^{\perp}$ satisfy $\min\{d_0^{'} + d_\mu^{'}, d^*\} \leq (d_2)_f^{\perp} \leq d^*$ and $(d_2)_f \geq (d^{\perp})^*$, where $d_0^{'}$ is the minimum distance of the code $C_0^{'}$ with parity check matrix $H_0^{'}$ and $d_\mu^{'}$ is the minimum distance of the code with parity check matrix $\tilde{H}_\mu^{'}$. The degree γ_2 of V_2 equals $\gamma_2 = \mu(\mathrm{rk}\, H_\mu^{'}) + \sum_{i=1}^{\mu-1}(\mu - i)[\mathrm{rk}\, H_{(\mu-i)}^{'} - \mathrm{rk}\, H_{(\mu-i+1)}^{'}]$; the code $V_2^{\perp}$ also has degree γ_2. On the other hand, the degree γ_1 of V_1 is equal to $\gamma_1 = \mu(\mathrm{rk}\, H_\mu + \mathrm{rk}\, H_\mu^{'}) + \sum_{i=1}^{\mu-1}(\mu - i)[\mathrm{rk}\, H_{(\mu-i)}^{'} - \mathrm{rk}\, H_{(\mu-i+1)}^{'}]$; $V_1^{\perp}$ also has degree γ_1.

We know that $V_2 \subset V_1$. The corresponding CSS-type code derived from V_1 and V_2 has frame size n, $k = \mathrm{rk}\, H_0$ logical qudits per frame, degree $\gamma = \gamma_1 + \gamma_2$, $(d_x)_f \geq (d_1)_f \geq d^{\perp}$ and $(d_z)_f \geq (d_2)_f^{\perp}$, where $\min\{d_0^{'} + d_\mu^{'}, d^*\} \leq (d_2)_f^{\perp} \leq d^*$. Thus one can get an $[(n, \mathrm{rk}\, H_0, \mu^*; \gamma_1 + \gamma_2, (d_z)_f/(d_x)_f)]_q$ AQCC. If $H_1(D)$ is a generator matrix of the code $V_1^{\perp}$ then a stabilizer matrix of our AQCC is given by

$$\left(\begin{array}{c|c} G_2(D) & 0 \\ 0 & H_1(D) \end{array} \right).$$

Other variant of this construction can be obtained by considering a CSS-type code derived from the pair of classical convolutional codes $V_1^{\perp} \subset V_2^{\perp}$. The proof is complete. □

3.2 Construction II

Let q be a prime power and n a positive integer such that $\gcd(q, n) = 1$. Let α be a primitive n-th root of unity in some extension field. Recall that a cyclic code C of length n over $\mathbb{F}_q$ is a Bose-Chaudhuri-Hocquenghem (BCH) code with designed distance δ if, for some integer $b \geq 0$, we have $g(x) = \mathrm{l.c.m.}\{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\}$, *i.e.*, $g(x)$ is the monic polynomial of smallest degree over F_q having $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros. Therefore,

$c \in C$ if and only if $c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+\delta-2}) = 0$. Thus the code has a string of $\delta - 1$ consecutive powers of α as zeros. It is well known that the minimum distance of a BCH code is greater than or equal to its designed distance δ. A parity check matrix for C is given by

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{(b+1)} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \cdots & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix},$$

where each entry is replaced by the corresponding column of l elements from $\mathbb{F}_q$, where $l = \mathrm{ord}_n(q)$, and then removing any linearly dependent rows. The rows of the resulting matrix over $\mathbb{F}_q$ are the parity checks satisfied by C.

Let us recall a useful results shown in [18]:

Theorem **3.2** *[18, Theorem 4.2] Assume that $q = 2^t$, where $t \geq 3$ is an integer, $n = q+1$ and consider that $a = \frac{q}{2}$. Then there exist classical MDS convolutional codes with parameters $(n, n-2i, 2; 1, 2i+3)_q$, where $1 \leq i \leq a-1$.*

Theorem 3.3 establishes conditions in which it is possible to construct AQCC's derived from BCH codes.

Theorem **3.3** *Let $q = 2^t$, where $t \geq 4$ and consider that $n = q+1$ and $a = \frac{q}{2}$. Then there exists an AQCC with parameters $[(n, 2i-4, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$, where $(d_z)_f \geq n-2i-1$ and $(d_x)_f \geq 3$, for all $3 \leq i \leq a-1$.*

Proof: Consider the parity check $\mathbb{F}_q$-matrix of the BCH code C given by

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha^a & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

whose entries are expanded with respect to some $\mathbb{F}_q$-basis $\mathcal{B}$ of $\mathbb{F}_{q^2}$, after removing the linearly dependent rows. This BCH code was constructed in the proof of [18, Theorem 4.2] (more precisely, it is the code C_2 constructed there); C is a MDS code with parameters $[n, n-2i-2, 2i+3]_q$. Its (Euclidean) dual code $C^\perp$ is also a MDS code with parameters $[n, 2i+2, n-2i-1]_q$.

Next, we construct a classical convolutional code V_1 generated by the reduced

basic matrices

$$G_1(D) = \begin{bmatrix} 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \dots & \alpha^{(n-1)(a-i+2)} \\ - & - & - & - & - \\ 1 & \alpha^{a} & \dots & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \dots & \dots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+3)} & \alpha^{2(a-i+3)} & \dots & \alpha^{(n-1)(a-i+3)} \end{bmatrix} + \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \\ - & - & - & - & - \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \dots & \alpha^{(n-1)(a-i)} \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} D$$

and

$$G_2(D) = \begin{bmatrix} 1 & \alpha^{(a-i+2)} & \alpha^{2(a-i+2)} & \dots & \alpha^{(n-1)(a-i+2)} \end{bmatrix} + \begin{bmatrix} 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \dots & \alpha^{(n-1)(a-i+1)} \end{bmatrix} D$$

The code V_1, generated by $G_1(D)$, is a unit memory code of dimension $k_1 = 2(i-1)$ and degree $\gamma_1 = 4$; V_1 is an $(n, 2[i-1], 4; 1, [d_1]_f \geq n-2i-1)_q$ code. Its Euclidean dual code $V_1^{\perp}$ has parameters $(n, n-2[i-1], 4; \mu_1^{\perp}, [d_1]_f^{\perp} \geq 2i+2)_q$. The code V_2, generated by $G_2(D)$, is an $(n, 2, 2; 1, [d_2]_f)_q$ code, so $V_2^{\perp}$ has parameters $(n, n-2, 2; \mu_2^{\perp}, [d_2]_f^{\perp} \geq 3)_q$. From construction, it follows that $V_2 \subset V_1$, so $V_1^{\perp} \subset V_2^{\perp}$. Consider the stabilizer matrix given by

$$\left(\begin{array}{c|c} H_1(D) & 0 \\ 0 & G_2(D) \end{array} \right),$$

where $H_1(D)$ is a parity check matrix of the code $V_1^{\perp}$. The corresponding CSS-type code has $K = 2i-4$, $\gamma = 6$, $(d_z)_f \geq n-2i-1$ and $(d_x)_f \geq 3$. Thus there exists an $[(n, 2i-4, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$ AQCC. □

Remark **3.4** *It is interesting to note that the idea of construction of the matrix $G_2(D)$ shown in the proof of Theorem 3.3 is distinct from that given in Theorem 3.1.*

Theorem **3.5** *Let $q = 2^l$, where $l \geq 4$ and consider that $n = q+1$ and $a = \frac{q}{2}$. Then there exist AQCC's with parameters*

a) $[(n, 2i-2t-2, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq n-2i-1$, $(d_x)_f \geq 2t+3$, *i and t are positive integers such that $1 \leq t \leq i-2$ and $3 \leq i \leq a-1$;*

b) $[(n, 2i-2t, \mu^*; 4, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq n-2i-1$, $(d_x)_f \geq 2t+3$, *i and t are positive integers such that $1 \leq t \leq i-1$ and $2 \leq i \leq a-1$.*

Proof: We only show Item a), since Item b) is similar. The notation and the matrix $\mathcal{H}$ is the same as in the proof of Theorem 3.3. We split $\mathcal{H}$ into disjoint submatrices in order to construct a reduced basic generator matrix $G_1(D)$ of the code V_1, given by

$$G_1(D) = \begin{bmatrix} 1 & \alpha^{[a-(t+1)]} & \alpha^{2[a-(t+1)]} & \cdots & \alpha^{(n-1)[a-(t+1)]} \\ 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{[a-(t-1)]} & \alpha^{2[a-(t-1)]} & \cdots & \alpha^{(n-1)[a-(t-1)]} \\ - & - & - & - & - \\ 1 & \alpha^{[a-(t+2)]} & \alpha^{2[a-(t+2)]} & \cdots & \alpha^{(n-1)[a-(t+2)]} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{[a-(i-2)]} & \alpha^{2[a-(i-2)]} & \cdots & \alpha^{(n-1)[a-(i-2)]} \\ 1 & \alpha^{[a-(i-1)]} & \alpha^{2[a-(i-1)]} & \cdots & \alpha^{(n-1)[a-(i-1)]} \end{bmatrix} + \\ \begin{bmatrix} 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \\ 1 & \alpha^{(a-t)} & \alpha^{2(a-t)} & \cdots & \alpha^{(n-1)(a-t)} \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \\ - & - & - & - & - \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} D,$$

Let V_2 be the convolutional code generated by the reduced basic matrix $G_2(D)$

$$G_2(D) = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{[a-(t-1)]} & \alpha^{2[a-(t-1)]} & \cdots & \alpha^{(n-1)[a-(t-1)]} \end{bmatrix} + \\ \begin{bmatrix} 1 & \alpha^{(a-t)} & \alpha^{2(a-t)} & \cdots & \alpha^{(n-1)(a-t)} \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} D$$

It is easy to see that the code V_1 has parameters $(n, 2i-2, 4; 1, [d_1]_f \geq n-2i-1)_q$ and $V_1^{\perp}$ has parameters $(n, n-2i+2, 4; \mu_1^{\perp}, [d_1]_f^{\perp})_q$. The code V_2, generated by $G_2(D)$, is an $(n, 2t, 2; 1, [d_2]_f)_q$ code, so $V_2^{\perp}$ has parameters $(n, n-2t, 2; \mu_2^{\perp}, [d_2]_f^{\perp} \geq 2t+3)_q$. Since $V_2 \subset V_1$, it follows that $V_1^{\perp} \subset V_2^{\perp}$. Thus there exists an $[(n, 2i-2t-2, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$ AQCC, where $(d_z)_f \geq n-2i-1$ and $(d_x)_f \geq 2t+3$. □

Example **3.1** *Applying Theorem 3.5, one can get AQCC's with parameters* $[(17,6,\mu^*;6,[d_z]_f \geq 6/[d_x]_f \geq 5)]_{16}$, $[(17,8,\mu^*;4,[d_z]_f \geq 6/[d_x]_f \geq 5)]_{16}$, $[(17,8,\mu^*;6,[d_z]_f \geq 5/[d_x]_f \geq 4)]_{16}$, $[(17,10,\mu^*;4,[d_z]_f \geq 5/[d_x]_f \geq 4)]_{16}$, $[(33,24,\mu^*;6,[d_z]_f \geq 5/[d_x]_f \geq 4)]_{32}$, $[(33,26,\mu^*;4,[d_z]_f \geq 5/[d_x]_f \geq 4)]_{32}$, $[(33,22,\mu^*;6,[d_z]_f \geq 6/[d_x]_f \geq 5)]_{32}$, $[(33,24,\mu^*;4,[d_z]_f \geq 6/[d_x]_f \geq 5)]_{32}$, $[(33,20,\mu^*;6,[d_z]_f \geq 8/[d_x]_f \geq 5)]_{32}$, $[(33,22,\mu^*;4,[d_z]_f \geq 8/[d_x]_f \geq 5)]_{32}$ *and so on.*

Theorem **3.6** *Assume that* $q = p^l$, *where* p *is an odd prime and* $l \geq 2$. *Consider that* $n = q+1$ *and* $a = \frac{n}{2}$. *Then there exist AQCC's with parameters*

a) $[(n, 2i-2t-2, \mu^*; 6, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq n-2i$ *and* $(d_x)_f \geq 2t+2$, *for all* $1 \leq t \leq i-2$, *where* $3 \leq i \leq a-1$;

b) $[(n, 2i-2t, \mu^*; 4, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq n-2i$ *and* $(d_x)_f \geq 2t+2$, *for all* $1 \leq t \leq i-1$, *where* $2 \leq i \leq a-1$.

Proof: Analogous to that of Theorem 3.5. □

Remark **3.7** *One more time we call the attention that the idea of construction of the matrix* $G_2(D)$ *is different for each of Theorems 3.1, 3.3, 3.5 and 3.6. This remark also holds for the results shown in Subsection 3.3.*

3.3 Construction III

In this subsection we are interested in constructing AQCC's derived from Reed-Solomon (RS) and generalized Reed-Solomon (GRS) codes. We first deal with RS codes. Recall that a RS code over $\mathbb{F}_q$ is a BCH code, of length $n = q-1$, with parameters $[n, n-d+1, d]_q$, where $2 \leq d \leq n$. A parity check matrix of a RS code is given by

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{(b+1)} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(b+d-2)} & \cdots & \cdots & \alpha^{(n-1)(b+d-2)} \end{bmatrix},$$

whose entries are in $\mathbb{F}_q$.

In Theorem 3.8 presented in the following, we construct AQCC's derived from RS codes:

Theorem **3.8** *Assume that* $q \geq 8$ *is a prime power. Then there exist AQCC's with parameters*

a) $[(q-1, i-t-1, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq q-i-1$, $(d_x)_f \geq t+2$, *for all* $1 \leq t \leq i-2$, *where* $3 \leq i \leq q-3$;

b) $[(q-1, i-t, \mu^*; 2, [d_z]_f/[d_x]_f)]_q$, *where* $(d_z)_f \geq q-i-1$, $(d_x)_f \geq t+2$, *for all* $1 \leq t \leq i-1$, *where* $2 \leq i \leq q-3$.

Proof: We only show Item a), since Item b) is similar. The construction is the same as in the proof of Theorem 3.5, although the codes have distinct parameters. More specifically, starting from a parity check matrix $\mathcal{H}$

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha^{a} & \cdots & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{(a-1)} & \cdots & \cdots & \alpha^{(n-1)(a-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{(a-i+1)} & \alpha^{2(a-i+1)} & \cdots & \alpha^{(n-1)(a-i+1)} \\ 1 & \alpha^{(a-i)} & \alpha^{2(a-i)} & \cdots & \alpha^{(n-1)(a-i)} \end{bmatrix},$$

of an $[q-1, q-i-2, i+2]_q$ RS code, we construct generator matrices $G_1(D)$ and $G_2(D)$ for codes V_1 and V_2, respectively as per Theorem 3.5. In this context, it is easy to see that V_1 is an $(q-1, i-1, 2; 1, [d_1]_f \geq q-i-1)_q$ code, $V_1^{\perp}$ is an $(q-1, q-i, 2; \mu_1^{\perp}, [d_1]_f^{\perp})_q$ code, V_2 is an $(q-1, t, 1; 1, [d_2]_f)_q$ and $V_2^{\perp}$ an $(q-1, q-t-1, 1; \mu_2^{\perp}, [d_1]_f^{\perp} \geq t+2)_q$. Then the corresponding CSS-type code has parameters $[(q-1, i-t-1, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$, where $(d_z)_f \geq q-i-1$ and $(d_x)_f \geq t+2$. □

Example **3.2** *By means of Theorem 3.8, one can construct AQCC's with parameters* $[(10, 4, \mu^*; 3, [d_z]_f \geq 4/[d_x]_f \geq 3)]_{11}$, $[(10, 5, \mu^*; 3, [d_z]_f \geq 3/[d_x]_f \geq 3)]_{11}$, $[(10, 2, \mu^*; 3, [d_z]_f \geq 6/[d_x]_f \geq 3)]_{11}$, $[(10, 1, \mu^*; 3, [d_z]_f \geq 6/[d_x]_f \geq 4)]_{11}$, *and so on.*

Let us recall the definition of GRS codes. Let n be an integer such that $1 \leq n \leq q$, and choose an n-tuple $\zeta = (\zeta_0, \ldots, \zeta_{n-1})$ of distinct elements of $\mathbb{F}_q$. Assume that $\mathbf{v} = (v_0, \ldots, v_{n-1})$ is an n-tuple of nonzero (not necessary distinct) elements of $\mathbb{F}_q$. For any integer k, $1 \leq k \leq n$, consider the set of polynomials of degree less than k, in $\mathbb{F}_q[x]$, denoted by $\mathcal{P}_k$. Then we define the GRS codes as $\mathrm{GRS}_k(\zeta, \mathbf{v}) = \{(v_0 f(\zeta_0), v_1 f(\zeta_1), \ldots, v_{n-1} f(\zeta_{n-1})) | f \in \mathcal{P}_k\}$. It is well known that $\mathrm{GRS}_k(\zeta, \mathbf{v})$ is a MDS code with parameters $[n, k, n-k+1]_q$. The (Euclidean) dual $\mathrm{GRS}_k^{\perp}(\zeta, \mathbf{v})$ of $\mathrm{GRS}_k(\zeta, \mathbf{v})$ is also a GRS code and $\mathrm{GRS}_k^{\perp}(\zeta, \mathbf{w}) = \mathrm{GRS}_{n-k}(\zeta, \mathbf{v})$ for some n-tuple $\mathbf{w} = (w_0, \ldots, w_{n-1})$ of nonzero elements of $\mathbb{F}_q$. A generator matrix of $\mathrm{GRS}_k(\zeta, \mathbf{v})$ is given by

$$G = \begin{bmatrix} v_0 & v_1 & \cdots & v_{n-1} \\ v_0\zeta_0 & v_1\zeta_1 & \cdots & v_{n-1}\zeta_{n-1} \\ v_0\zeta_0^2 & v_1\zeta_1^2 & \cdots & v_{n-1}\zeta_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_0\zeta_0^{k-1} & v_1\zeta_1^{k-1} & \cdots & v_{n-1}\zeta_{n-1}^{k-1} \end{bmatrix};$$

a parity check matrix of $\mathrm{GRS}_k(\zeta, \mathbf{v})$ is

$$H = \begin{bmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\zeta_0 & w_1\zeta_1 & \cdots & w_{n-1}\zeta_{n-1} \\ w_0\zeta_0^2 & w_1\zeta_1^2 & \cdots & w_{n-1}\zeta_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ w_0\zeta_0^{n-k-1} & w_1\zeta_1^{n-k-1} & \cdots & w_{n-1}\zeta_{n-1}^{n-k-1} \end{bmatrix}.$$

In the next result, we construct new AQCC's derived from GRS codes.

Theorem **3.9** *Let $q \geq 5$ be a prime power. Assume that $k \geq 1$ and $n \geq 5$ are integers such that $n \leq q$ and $k \leq n-4$. Choose an n-tuple $\zeta = (\zeta_0, \ldots, \zeta_{n-1})$ of distinct elements of $\mathbb{F}_q$ and an n-tuple $\mathbf{v} = (v_0, \ldots, v_{n-1})$ of nonzero elements of $\mathbb{F}_q$. Then there exists an $[(n, n-t-k-2, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$ AQCC, where $(d_z)_f \geq t+2$ and $(d_x)_f \geq k+1$, $1 \leq t \leq n-k-2$.*

Proof: Let

$$H = \begin{bmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\zeta_0 & w_1\zeta_1 & \cdots & w_{n-1}\zeta_{n-1} \\ w_0\zeta_0^2 & w_1\zeta_1^2 & \cdots & w_{n-1}\zeta_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ w_0\zeta_0^{n-k-1} & w_1\zeta_1^{n-k-1} & \cdots & w_{n-1}\zeta_{n-1}^{n-k-1} \end{bmatrix}.$$

be a parity check matrix of an $\mathrm{GRS}_k(\zeta, \mathbf{v})$ code. We split H to form polynomial matrices $G_1(D)$ and $G_2(D)$ of codes V_1 and V_2, respectively, as follows:

$$G_1(D) = \begin{bmatrix} w_0\zeta_0^{n-k-3} & w_1\zeta_1^{n-k-3} & \cdots & w_{n-1}\zeta_{n-1}^{n-k-3} \\ w_0 & w_1 & \cdots & w_{n-1} \\ w_0\zeta_0 & w_1\zeta_1 & \cdots & w_{n-1}\zeta_{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ w_0\zeta_0^{t-1} & w_1\zeta_1^{t-1} & \cdots & w_{n-1}\zeta_{n-1}^{t-1} \\ - & - & - & - \\ w_0\zeta_0^{t+1} & w_1\zeta_1^{t+1} & \cdots & w_{n-1}\zeta_{n-1}^{t+1} \\ \vdots & \vdots & \vdots & \vdots \\ w_0\zeta_0^{n-k-2} & w_1\zeta_1^{n-k-2} & \cdots & w_{n-1}\zeta_{n-1}^{n-k-1} \end{bmatrix} +$$

$$\begin{bmatrix} w_0\zeta_0^{n-k-1} & w_1\zeta_1^{n-k-1} & \cdots & w_{n-1}\zeta_{n-1}^{n-k-1} \\ w_0\zeta_0^{t} & w_1\zeta_1^{t} & \cdots & w_{n-1}\zeta_{n-1}^{t} \\ 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \\ - & - & - & - \\ 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \end{bmatrix} D$$

and

$$G_2(D) = \begin{bmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\zeta_0 & w_1\zeta_1 & \cdots & w_{n-1}\zeta_{n-1} \\ w_0\zeta_0^2 & w_1\zeta_1^2 & \cdots & w_{n-1}\zeta_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ w_0\zeta_0^{t-1} & w_1\zeta_1^{t-1} & \cdots & w_{n-1}\zeta_{n-1}^{t-1} \end{bmatrix} + \begin{bmatrix} w_0\zeta_0^t & w_1\zeta_1^t & \cdots & w_{n-1}\zeta_{n-1}^t \\ 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \end{bmatrix} D,$$

where $\mathbf{w} = (w_0, \ldots, w_{n-1})$ is a vector such that $\mathrm{GRS}_k^{\perp}(\zeta, \mathbf{w}) = \mathrm{GRS}_{n-k}(\zeta, \mathbf{v})$. The code V_1 has parameters $(n, n-k-2, 2; 1, [d_1]_f \geq k+1)_q$ and $V_1^{\perp}$ has parameters $(n, k+2, 2; \mu_1^{\perp}, [d_1]_f^{\perp})_q$. Similarly, V_2 is an $(n, t, 1; 1, [d_2]_f)_q$ code and $V_2^{\perp}$ is an $(n, n-t, 1; \mu_2^{\perp}, [d_1]_f^{\perp} \geq t+2)_q$ code. Then there exists an $[(n, n-t-k-2, \mu^*; 3, [d_z]_f/[d_x]_f)]_q$ code, where $(d_z)_f \geq t+2$ and $(d_x)_f \geq k+1$. □

Example **3.3** *From Theorem 3.9, we can construct AQCC's with parameters* $[(5, 1, \mu^*; 3, [d_z]_f \geq 3/[d_x]_f \geq 2)]_5$, $[(7, 1, \mu^*; 3, [d_z]_f \geq 4/[d_x]_f \geq 3)]_7$, $[(8, 1, \mu^*; 3, [d_z]_f \geq 5/[d_x]_f \geq 3)]_8$, $[(17, 7, \mu^*; 3, [d_z]_f \geq 7/[d_x]_f \geq 4)]_{17}$, $[(17, 7, \mu^*; 3, [d_z]_f \geq 6/[d_x]_f \geq 5)]_{17}$, $[(17, 6, \mu^*; 3, [d_z]_f \geq 7/[d_x]_f \geq 5)]_{17}$, $[(17, 4, \mu^*; 3, [d_z]_f \geq 9/[d_x]_f \geq 5)]_{17}$ *and so on.*

Theorem **3.10** *Let $q \geq 5$ be a prime power. Assume that $k \geq 1$ and $n \geq 5$ are integers such that $n \leq q$ and $k \leq n-4$. Choose an n-tuple $\zeta = (\zeta_0, \ldots, \zeta_{n-1})$ of distinct elements of $\mathbb{F}_q$ and an n-tuple $\mathbf{v} = (v_0, \ldots, v_{n-1})$ of nonzero elements of $\mathbb{F}_q$. Then an $[(n, n-t-k-1, \mu^*; 2, [d_z]_f/[d_x]_f)]_q$ AQCC, where $(d_z)_f \geq t+2$, $(d_x)_f \geq k+1$ and $1 \leq t \leq n-k-1$ can be constructed.*

Proof: Similar to that of Theorem 3.9. □

Example **3.4** *From Theorem 3.10, we obtain AQCC's with parameters* $[(5, 1, \mu^*; 2, [d_z]_f \geq 4/[d_x]_f \geq 2)]_5$, $[(7, 2, \mu^*; 2, [d_z]_f \geq 4/[d_x]_f \geq 3)]_7$, $[(7, 2, \mu^*; 2, [d_z]_f \geq 5/[d_x]_f \geq 2)]_7$, $[(7, 1, \mu^*; 2, [d_z]_f \geq 5/[d_x]_f \geq 3)]_7$.

4 Discussion

Our main result is Theorem 3.1, which establishes a general technique of construction for AQQC's. Subsection 3.2 is concerned with constructions of AQQC's derived from classical MDS-convolutional BCH codes and, in Subsection 3.3, we address the construction of AQQC's derived from classical Reed-Solomon and

generalized Reed-Solomon convolutional codes. It is interesting to note that the choice of matrices $G_1(D)$ and $G_2(D)$ was based on the fact that the corresponding (classical) convolutional codes must be non-catastrophic, with great dimension and minimum distances.

As was mentioned previously, this is the first work available in literature dealing with constructions of asymmetric quantum convolutional codes. Moreover, by applying algebraic techniques, we have derived several families of such codes, and not only few codes with specific parameters. However, much research remains to be done in the area of AQCC's. In fact, there is no bound for the respective free distances nor relationships among the parameters of AQCC's. Other impossibility is to compare the parameters of the new AQCC's with the ones displayed in literature, i.e., our codes have parameters quite distinct of the QCC's available in literature. This area of research needs much investigation, since it was introduced recently (see [25]) in literature. Additionally, even in the case of constructions of good QCC's, only few works are displayed in literature [7, 3, 18, 19]. Moreover, the unique bound known in literature even for QCC's is the generalized quantum Singleton bound (GQSB), introduced by Klappenecker *et al.* (see [3]).

For future works, it will be interesting to establish analogous results to (asymmetric) quantum generalized Singleton bound (see [3]), the (asymmetric) sphere packing bound among other.

5 Summary

We have constructed the first families of asymmetric quantum convolutional codes available in literature. These new AQCC's are derived from suitable families of classical convolutional codes with good parameters, which have been also constructed in this paper. Our codes have great asymmetry. Additionally, great variety of distinct types of codes have also been presented. However, much work remains to be done in order to find bounds for AQCC's as well as for the development of such area of research.

Acknowledgment

This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

[1] A. C. A. de Almeida and R. Palazzo Jr.. A concatenated $[(4, 1, 3)]$ quantum convolutional code. In *Proc. IEEE Inform. Theory Workshop (ITW)*, pp. 28–33, 2004.

[2] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, P. K. Sarvepalli. Quantum convolutional BCH codes. e-print arXiv:quant-ph/0703113.

[3] S. A. Aly, A. Klappenecker, P. K. Sarvepalli. Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes. e-print arXiv:quant-ph/0701037.

[4] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[6] G. D. Forney Jr. Convolutional codes I: algebraic structure. *IEEE Trans. Inform. Theory*, 16(6):720–738, 1970.

[7] G. D. Forney Jr., M. Grassl, S. Guha. Convolutional and tail-biting quantum error-correcting codes. *IEEE Trans. Inform. Theory*, 53(3):865–880, 2007.

[8] M. Grassl and M. Rötteler. Non-catastrophic encoders and encoder inverses for quantum convolutional codes. In *Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1109–1113, 2006.

[9] M. Grassl and M. Rötteler. Constructions of quantum convolutional codes. e-print arXiv:quant-ph/0703182.

[10] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* University Press, Cambridge, 2003.

[11] L. Ioffe and M. Mezard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345(1–4), 2007.

[12] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding.* Digital and Mobile Communication, Wiley-IEEE Press, 1999.

[13] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[14] G. G. La Guardia. Constructions of new families of nonbinary quantum codes. *Phys. Rev. A*, 80(4):042331(1–11), 2009.

[15] G. G. La Guardia. New quantum MDS codes. *IEEE Trans. Inform. Theory*, 57(8):5551–5554, 2011.

[16] G. G. La Guardia. Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes. *Quantum Inform. Processing*, 11(2):591–604, 2012.

[17] G. G. La Guardia. Asymmetric quantum codes: new codes from old. *Quantum Inform. Processing*, 12:2771–2790, 2013.

[18] G. G. La Guardia. On classical and quantum MDS-convolutional BCH codes. *IEEE Trans. Inform. Theory*, 60(1):304–312, 2014.

[19] G. G. La Guardia. On negacyclic MDS-convolutional codes. *Linear Algebra and its Applic.*, (448):85–96, 2014.

[20] L. N. Lee. Short unit-memory byte-oriented binary convolutional codes having maximum free distance. *IEEE Trans. Inform. Theory*, 22:349–352, 1976.

[21] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.

[22] H. Gluesing-Luerssen, W. Schmale. Distance bounds for convolutional codes and some optimal codes. e-print arXiv:math/0305135.

[23] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[25] H. Ollivier and J.-P. Tillich. Description of a quantum convolutional code. *Phys. Rev. Lett.*, 91(17):1779021–4, 2003.

[26] H. Ollivier and J.-P. Tillich. Quantum convolutional codes: fundamentals. e-print arXiv:quant-ph/0401134.

[27] Ph. Piret. *Convolutional Codes: An Algebraic Approach.* Cambridge, Massachusetts: The MIT Press, 1988.

[28] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Applicable Algebra in Eng. Comm. Comput.*, 10:15–32, 1998.

[29] P. K. Sarvepalli, A. Klappenecker, M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. In *Proc. of the Royal Society A*, pp. 1645–1672, 2009.

[30] R. Smarandache, H. G.-Luerssen, J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.

[31] A. M. Steane. Simple quantum error correcting-codes. *Phys. Rev. A*, 54:4741–4751, 1996.